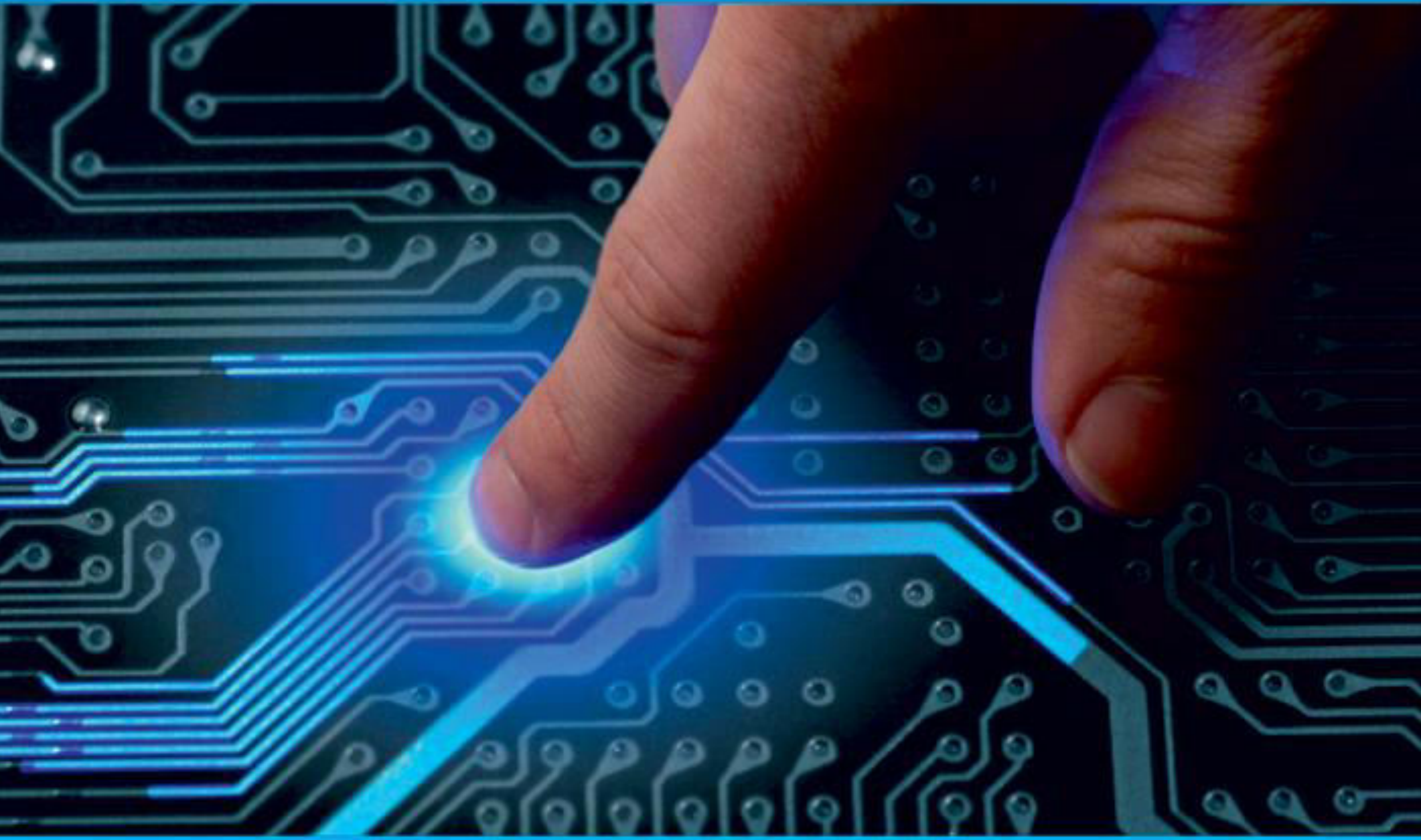
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 10, October 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910009 |

CLOUD COMPUTING SECURITY

L.Subhashini[1], Ms.S.Maheswari[2], Dr.D.Karthikeswaran[3]

PG Scholar, Department of Computer Science and Engineering, Nandha Engineering College, Erode, Tamil Nadu, India[1]

Assistant Professor, Department of Computer Science and Engineering, Nandha Engineering College, Erode, Tamil Nadu, India[2]

Professor, Department of Computer Science and Engineering, Nandha Engineering College, Erode, Tamil Nadu, India[3]

ABSTRACT: Cloud computing is an emerging paradigm that aims to provide computing resources, massive data storage capacity and, flexible data sharing services. Data must be encrypted prior to storing it in the, potentially untrustworthy cloud. Existing traditional encryption systems impose a heavy burden of managing files and encryption operations on data owners. They suffer from serious security, efficiency, and usability issues, and some schemes are in appropriate for protecting cloud data. In this paper, we introduce OutFS, a user-side encrypted file system, focused on providing a transparent encryption for stored and shared outsourced data. In OutFS, we utilize a hybrid encryption scheme structure based on symmetric and asymmetric methods. The key management is conveniently designed. In order to ensure robust data sharing security, the identity-based encryption scheme (IBE) is integrated with OutFS. OutFS is designed to preserve the integrity of outsourced file data and file system data structure. Analysis of performance and experimental results show that OutFS is efficient. It can achieve an average throughput of 8.8 MB/sec, and 10.5 MB/sec for writing and reading outsourced files. Security analysis indicates that OutFS is extremely secure and robust against attacks such as brute-force, eavesdropping, man-in-the-middle, and offline-dictionary attacks

KEYWORDS: Secure outsourced data, cloud computing security, encryption file system, transparent encryption, secure data sharing.

I. INTRODUCTION

The rapid development of cloud computing, more cloud services are into our daily life, and thus security protection of cloud services, especially data privacy protection, becomes more important. However to perform privacy protection causes huge overhead. Thus it is a critical issue to perform the most suitable protection to decline performance consumption while provide privacy protection.

1.1 CLOUD MODELS:

There are three types of models present in cloud computing which are given as follows:

Public Cloud Model: The public cloud model is defined as a cloud infrastructure which is managed by an organization providing third-party service. This is available as a service over the internet for both individual users and software companies/ organizations. This model's main advantage is that it is very large in scale. With limited configurations and security protection, the users in this model share the same infrastructure pool as provided by the service provider.

Private Cloud Model: The private cloud model is defined as a cloud computing infrastructure exclusively developed by a given company for each project or software. This requires a policy of permission to host cloud applications to enforce system security and control. In addition to being generated for each specific project, an external party or supplier also provide the cloud service.

Hybrid Cloud Model: The hybrid cloud model is defined as a cloud computing infrastructure that combines both public and private cloud models' advantageous factors. This is done using separate algorithms used to switch between the two infrastructures.

1.2 CLOUD COMPUTING MODELS

Infrastructure as a service (IaaS) allows users to use their storage or computational units remotely to access the given network. It does soon a demand-based basis whenever the service is required by the user. E.g: Microsoft Azure, Amazon Web Service.

Platform as a Service (PaaS) enables users to quickly and easily create web applications with permissions to provide a substitute for the purchase and maintenance of the system's software and infrastructure. Eg: Google App Engine.
Software as a service (SaaS) enables users to obtain an application license for any user, either as an ondemand service or through Internet subscription. In a simple way, it can be rented for use in a pay-as-you-go way instead of buying the required software. Example: Sales force, Cisco WebEx.

1.3. CLOUD COMPUTING TOOLS

Cloud services across a network are used as efficient, organizational-based business solutions. Various cloud computing tools, such as Eucalyptus, Open Nebula, Nimbus, Open stack, ete., are available where they all have different deployment strategies.
Cloud computing load balancing is defined as the process of distributing workload and computing resources within a networked cloud computing environment. It enables an organization to manage applications or workload demands on a task-by-task basis, by allocating resources on the networks between the various computers or through servers.

1.4DATA PRODUCTION:

The privacy levels are divided into two levels speed and security are implemented. In this aspect, some of the document or text file is splitted into two segments and first one is encrypted by 3DES and second one is encrypted by AES encryption mechanism. This reduces the processing and communication overhead.It not only fulfills the user-demand privacy but also maintains the cloud system performance in different cloud environments.

II. LITERATURE SURVEY

Ramkumar, K. and Gunasekaran, G. [1], Preserving security using crisscross AES and FCFS scheduling in cloud computing**,** Cloud computing is a developing technology in distributed computing which provides pay service model as per user need and requirement. Cloud includes the collection of virtual machine which have both computational and storage facility. The objective of cloud computing is to provide effective process to hyper distributed resources.A scheduling algorithm of collocate first come first server (FCFS) of supremacy elements is proposed where the system efficiency is improved using FCFS in parallel manner. FCFS is simple and fast. To address security problem, crisscross advance encryption standard (AES) is proposed by increasing the security in the cloud through the grid manner. AES uses an identical key for both encrypting and decrypting the text.

Yenumula B Reddy[2], Cloud-Based Cyber Physical Systems Design Challenges and Security Needs,The cyber-physical systems are the combination of computational elements and physical entities that can interact with humans through many modalities. The research in cyber physical systems is in its initial stage. Therefore, first we discussed the status of security in cloud cyber-physical systems. Second, we introduced the challenges ahead to the design and development of the future engineering systems with new security capabilities. Third, we presented the security requirements in Hadoop distributed file systems.

Satish Kumar and Anita Ganpati [3], New Enhanced Techniques for security in cloud computing, Cloud computing has a lot of security issues that are gaining great attention nowadays, including the data protection, network security, virtualization security, application integrity, and identity management.The most popular security techniques include SSL (Secure Socket Layer) Encryption, Intrusion Detection System; Multi Tenancy based Access Control, etc. Goal of this paper is to analyze and evaluate the most important security techniques for data protection in cloud computing.
Ali ShokrollahiYancheshmeh[4], Multi-Tenancy Security in Cloud Computing, Cloud computing has enabled small organizations to build web and mobile apps for millions of users by utilizing the concept of "pay-as-you-go" for applications, computing, network and storage resources as on-demand services. These services can be provided to the tenants in different categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).Since Multi-Tenancy dramatically depends on resource sharing, many experts have suggested different approaches to secure Multi-Tenancy. One of the solutions is resource allocation and isolation techniques. OpenStack community uses a method to isolate the resources in a Multi-Tenant environment.

Ren, Yulong, and Wen Tang[5], Security with BIG DATA in Cloud Computing,In recent years, big data and cloud computing are the major issues in an organizations. It enables computing resources to be provided as information technology service with high efficiency and effectiveness. Today's big data is the one of the major problem that researchers try to solve it. The main focus is on security issues in cloud computing that are associated with big data. Big data applications are a great benefit to organizations, business, companies and many large scale and small scale industries. The possible solutions for the issues in cloud computing security and Hadoop

Thabit, A.P.S. Alhomdy, A.H.A. Al-Ahdal et al[6], A New Lightweight Cryptographic Algorithm for Enhancing Data Security in Cloud Computing, Data has been pivotal to all facets of human life in the last decades. In recent years, the massive growth of data as a result of the development of various applications. This data needs to be secured and stored in secure sites. Cloud computing is the technology can be used to store those massive amounts of data. New Lightweight Cryptographic Algorithm for Enhancing Data Security that can be used to secure applications on cloud computing. The algorithm is a 16 bytes (128-bit) block cipher and wants 16 bytes (128-bit) key to encrypt the data. It is inspired by feistal and substitution permutation architectural methods to improve the complexity of the encryption.

SrijitaBasu[8], Cloud computing security challenges & solutions-A survey, Cloud Computing and its' related security issues as well as countermeasures are one of the highly debated topics in today's research field. Though, various surveys regarding Cloud security are already prevalent, there remains a certain gap between the proper mapping of these issues to their corresponding solutions.Some surveys present the Virtualization issues and solutions while other deal with the access control mechanisms, but what lacks is a common framework that would at the same time generalize the concept of cloud security as well as intricately analyze its' specific requirements.

Antonio Celesti, Francesco Tusa, Massimo Villari and Antonio Puliafito[9], Security and Cloud Computing InterCloud Identity Management Infrastructure, Cloud Computing is becoming one of the most important topics in the IT world. Several challenges are being raised from the adoption of this computational paradigm including security, privacy, and federation. This paper aims to introduce new concepts in cloud computing and security, focusing on heterogeneous and federated scenarios. We present reference architecture able to address the Identity Management (IdM) problem in the InterCloud context and show how it can be successfully applied to manage the authentication needed among clouds for the federation establishment.

Wajid Hassan[10], Latest trends, challenges and Solutions in Security in the era of Cloud Computing and Software Defined Networks, Cloud computing has a potential of providing elastic, easily manageable, powerful and cost-effective solutions. Integrated security solutions should be devised to deal with the increasing security risks. The rapid transition to cloud computing has fueled concerns on the security issues. Attempts to evaluate various security threats to cloud computing and a number of security solutions have also been discussed. Furthermore, a brief view of the cloud security regulatory bodies and compliance have also been presented.

Eduardo B. Fernandez[10], Patterns for Security and Privacy in Cloud Ecosystems, An ecosystem is the expansion of a software product line architecture to include systems outside the product which interact with the product. We model here the architecture of a cloud- based ecosystem, showing security patterns for its main components. We discuss the value of this type of models.

HussainAlJahdali, AbdulazizAlbatli[11],Multi-tenancy in Cloud Computing, Cloud Computing becomes the trend of information technology computational model, the Cloud security is becoming a major issue in adopting the Cloud where security is considered one of the most critical concerns for the large customers of Cloud (i.e. governments and enterprises).we will propose an attack model based on a threat model designed to take advantage of Multi-Tenancy situation only. Before that, a clear understanding of Multi-Tenancy, its origin and its benefits will be demonstrated. Also, a novel way on how to approach Multi-Tenancy will be illustrated. Finally, we will try to sense any suspicious behavior that may indicate to a possible attack model empirically from Google trace logs.

Remya Sivan and Zuriati Ahmad Zukarnain [12], Security and privacy in cloud-based E-Health system, Cloud based healthcare computing have changed the face of healthcare in many ways. The main advantages of cloud computing in healthcare are scalability of the required service and the provision to upscale or downsize the data storge, collaborating Artificial Intelligence (AI) and machine learning.The current paper examined various research studies to explore the utilization of intelligent techniques in health systems and mainly focused into the security and privacy issues in the current technologies. We focused on a thorough review of current and existing literature on different approaches and mechanisms used in e-Health to deal with security and privacy issues.

Pragati Chavan1, Pradeep Patil2[13], IaaS Cloud Security, Cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-breed business other delivery models, and a lack of security in this layer will certainly affect the other delivery models, i.e., PaaS, and SaaS that are built upon IaaS layer

| DOI: 10.15680/IJIRCCE.2021.0910009 |

Anuj Kumar Yadav[14], Cloud Data Security using Auditing Scheme, Cloud computing has emerged as one of the latest computing paradigm and is a growing technology for upcoming years. According to NIST Cloud computing is a model for convenient, on-demand network access to a large pool of computing resources.The Cryptographic techniques can be used in cloud to protect the data from attackers. Some of the existing cryptographic methods that ensure the security of cloud data. Auditing scheme is presented using cryptographic techniques and by using the auditing scheme based on the cryptography user data becomes more secure, that leads to enhancement of trust between the end user and cloud provider.

J. Rama Prabha, S. Prabakaran[15], Security in Cloud Health Care, Cloud computing plays vital role in various services to the users. The application of cloud computing includes usage in business, media transmission, banking, health care, military application, insurance, wireless communication, etc. One such application using Cloud computing is health care. The healthcare data processing and communication technology (HDCT) is building a constant and secured health care data processing and sharing Electronic Health Services (EHS) are regularly utilized by the needy, specialists, and social insurance experts to diminish medical service cost and give productive human services forms health cloud preserves the character-particular sensitive information for numerous purposes including biomedical research, medical health insurance groups, clinical statistics analysis, and many others.

Omar Achbarou, My Ahmed El kiram, and Salim El Bouanani[16],Securing Cloud Computing from Different Attacks Using Intrusion Detection Systems, Cloud computing is a new way of integrating a set of old technologies to implement a new paradigm that creates an avenue for users to have access to shared and configurable resources through internet on-demand.cloud computing environment requires some intrusion detection systems (IDSs) for protecting each machine against attacks. The aim of this work is to present a classification of attacks threatening the availability, confidentiality and integrity of cloud resources and services.

Osama Ahmed Khashan[17], Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System, The rapid development of cloud computing, more cloud services are into our daily life, and thus security protection of cloud services, especially data privacy protection, becomes more important. However to perform privacy protection causes huge overhead. Thus it is a critical issue to perform the most suitable protection to decline performance consumption while provide privacy protection. In this project, the privacy levels are divided into two levels speed and security are implemented. In this aspect, some of the document or text file is splitted into two segments and first one is encrypted by 3DES and second one is encrypted by AES encryption mechanism. This reduces the processing and communication overhead.

III. COMPARATIVE ANALYSIS

S.No	Title	Techniques & Mechanisms	Parameter Analysis	Future Work
1	Preserving security using crisscross AES and FCFS scheduling in cloud computing	First Come First Server (FCFS) and Advance Encryption Standard (AES)	High security and time reduction	Investigating the efficacy of other cryptography algorithm and implement parallel computing to increase their performance
2	Cloud-Based Cyber Physical Systems Design Challenges and Security Needs	Hadoop distributed file system	Pluggable security mechanism, Kerberos mechanism.	The current state of detection of rootkit virus and McAfee solution

3	New Enhanced Techniques for security in cloud computing	Encryption, Authentication processes, Authorization practices	data protection, cloud computing location	security challenges of data protection when using cloud computing must be appropriately solved and minimized
4	Multi-Tenancy Security in Cloud Computing	smart filtering technique	Host-based IDS and Network-based IDS	Using a new filter for nova-scheduler and compare it with Aggregate Instance Extra Specs Filter and Aggregate Multi Tenancy Isolation filters.To implement new filters for compute nodes, also implement new filters for the backend
5	Security With BIG DATA in Cloud Computing	Cloud Security Alliance	Map Reduce and Hadoop Distributed File System	More researches required to overcome the security of big data instead of current security algorithms and methods.
6	A New Lightweight Cryptographic Algorithm for Enhancing Data Security In Cloud Computing	New Lightweight Cryptographic Algorithm	Cipher type, Block size, security power.	The NLCA algorithm can be implemented in hardware
7	Cloud computing security challenges & solutions-A survey	Virtualization, Cloud Service Provider(CSP)	Confidentiality, Integrity, and Availability	The works based on Reputation systems (for CSP trust evaluation) and that of for user trust evaluation are some of the few in this domain, a rigorous study and research in this area is expected to be done in the near future
8	Security and Cloud Computing InterCloud Identity Management Infrastructure	Identity Management (IdM) problem	Heterogeneous and federated scenarios	We plan to study the performances of InterCloud Identity Management Infrastructure (ICIMI) Evaluating the amount of authentications and the identity provider (IdP) enrollments needed
9	Latest trends, challenges and Solutions in Security in the era of Cloud Computing and Software Defined Networks	multi-tenant technology, virtualization, web services and less expensive hardware	cost effective, storage issues	The public cloud's regulatory compliant procedures require organizations to implement and define clear guidelines on risk acceptance processes of cloud and cloud usage responsibility.

10	Patterns for Security and Privacy in Cloud Ecosystems	security patterns	Software ecosystems, systems security	showing how security and privacy constraints propagate across components
11	Multi-tenancy in Cloud Computing	resource allocation technique	Virtualization and Resource Sharing	Reconstruct the complete attack model with in depth analysis
12	Security and privacy in cloud-based E-Health system	identity-based secure and encrypted data-sharing technique	privacy and security of digital data.	privacy and security in Electronic Health Records (EHRs).
13	IaaS Cloud Security	Security Model for IaaS (SMI)	complex security challenges	Determines vulnerabilities and countermeasures.
14	Cloud Data Security using Auditing Scheme	cryptographic techniques	Secure Data storage	some enhancement can be done using which user can perform dynamic operations such as updating, deletion, insertion
15	Security in Cloud Health Care	Electronic Health Data Record (EHDR)	diagnostic analysis and decision making process	The Electronic Health Data Record is processed and transmitted in a secured and confidential environment by improving accuracy and efficiency using various encryption algorithms.
16	Securing Cloud Computing from Different Attacks Using Intrusion Detection Systems	Host based IDS (HIDS) and Network based IDS (NIDS).	Threads and Attacks on cloud	IDS integrates knowledge and behavior analysis to increases a cloud‘s security
17	Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System	Hybrid Encryption	Fast Run-time, secure data sharing and low cost	we intend to enhance the performance of OutFS using several improvement suggestions, such as parallel encryption, selective encryption, and intelligent cryptography.

IV. CONCLUSION

OutFS is a user-side encrypted file system that is implemented based on FUSE to secure outsourced files to cloud storage systems. It can enforce a secure file system mount over the cloud synchronized directory to perform a transparent encryption on per-file basis using per-file keys. OutFS does not introduce dependencies to the asymmetric encryption ciphers, but rather proposes a hybrid encryption scheme that combinesSymmetric and asymmetric method used to encrypt files and file keys, respectively, for the outsourced personal and shared files. In addition, OutFS uses the IBE scheme to facilitate the outsourced file sharing accessible only by authorized users with appropriate secret keys. OutFS can guarantee the integrity of the outsourced data files and the file system data structure against tampering and deletion attacks.The results showth at OutFS is reasonably efficient. With a block size of 4 KB, OutFS could achieve an average throughput of 8.8 MB/sec, and 10.5 MB/sec, respectively, for writing and reading outsourced files. Security analysis show that the proposed OutFS is highly secure, and it can effectively resist attacks, such as brute-force, eavesdropping, man-in-the-middle, offline dictionary, and collusion attacks on outsourced files.

REFERENCES

[1] Ramkumar, K. and Gunasekaran, G. (2019) 'Preserving security using crisscross AES and FCFS scheduling in cloud computing', Int. J. Advanced Intelligence Paradigms, Vol. 12, Nos. 1/2, pp.77–85.
[2] Yenumula B Reddy (2015) 'Cloud-based Cyber Physical Systems: Design Challenges and Security Needs', Grambling State University, Grambling, LA 71245, USA .
[3] Satish Kumar and Anita Ganpati, "New Enhanced Techniques for Security in Cloud Computing", International Journal of Computer Science & Engineering Technology (IJCSET),Vol. 5, Issue 4, pp. 295-303, Apr. 2016.
[4] Ali ShokrollahiYancheshmeh "Multi-Tenancy Security in Cloud Computing ", Degree project in information and communication technology, second cycle, 30 credits stockholm, Sweden 2019
[5] Ren, Yulong, and Wen Tang"Security With BIG DATA in Cloud Computing", nternational Conference on Emerging Trends in IOT & Machine Learning, 2018
[6]Thabit, A.P.S. Alhomdy, A.H.A. Al-Ahdal et al "A new lightweight cryptographic algorithm for enhancing data security in cloud computing", Global Transitions Proceedings 2 (2021) 91–99.
[7] SrijitaBasu "Cloud computing security challenges & solutions-A survey", Conference Paper · January 2018
[8] Antonio Celesti, Francesco Tusa, Massimo Villari and Antonio Puliafito ''SecurityandCloudComputing: Inter Cloud Identity Management Infrastructur'', in Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WET ICE · January 2017
[9] Wajid Hassan "Latest trends, challenges and solutions in security in the era of cloud computing and software defined networks", 2019 Indiana State University, 200 N 7th St, Terre Haute, IN 47809, United States.
[10] Eduardo B. Fernandez "Patterns for Security and Privacy in Cloud Ecosystems ", Florida Atlantic University, Boca Raton, FL, USA ed@cse.fau.edu
[11] HussainAlJahdali, AbdulazizAlbatli" Multi-Tenancy in Cloud Computing", 2016 IEEE 8th International Symposium on Service Oriented System Engineering
[12] Remya Sivan and Zuriati Ahmad Zukarnain "Security and Privacy in Cloud-Based E-Health System", Symmetry 2021, 13, 742. https://doi.org/10.3390/ sym13050742
[13] Pragati Chavan1, Pradeep Patil2 "IaaS Cloud Security ", 2016 International Conference on Machine Intelligence Research and Advancement
[14] Anuj Kumar Yadav "Cloud Data Security using Auditing Scheme ", International Journal of Computer Applications (0975 – 8887) Volume 156 – No 8, December 2016
[15] J. Rama Prabha, S. Prabakaran "Security in Cloud Health Care ", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-4, November 2019
[16] Omar Achbarou, My Ahmed El kiram, and Salim El Bouanani" Securing Cloud Computing from Different Attacks Using Intrusion Detection Systems ", in International Journal of Interactive Multimedia and Artificial Intelligence · January 2017
[17] Osama Ahmed Khashan "Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System", publication on November 18, 2020.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details